

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF VIRGINIA  
Harrisonburg Division

IN THE MATTER OF THE SEARCH OF  
ICLOUD INFORMATION ASSOCIATED  
WITH APPLE ID  
[THEWLOUNGEBAR@GMAIL.COM](mailto:THEWLOUNGEBAR@GMAIL.COM) AND  
IMEI 356707085318830 THAT IS STORED  
AT PREMISES CONTROLLED BY APPLE,  
INC.

Case No. 5:20mj00030

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Tami Ketcham, being duly sworn, depose and state the following:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at 1 Infinite Loop, Cupertino, California. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the United States Immigration and Customs Enforcement, Homeland Security Investigations (“HSI”), and have been since 2010. I am currently assigned to the HSI office in Harrisonburg, Virginia. I have a bachelor’s degree in Psychology and Sociology and a master’s degree in Criminology. I am authorized to conduct criminal investigations on behalf of HSI. During my employment with HSI, I have participated in the execution of subpoenas, search warrants, arrest warrants, interviews, and have investigated various federal violations,

including offenses pertaining to child exploitation and child pornography. Through such investigations, I have reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media. My duties include, but are not limited to, investigations pertaining to Title 18 of the United States Code. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program and have also received additional HSI investigative training, some of which has been related to conducting child exploitation and child pornography investigations. I previously worked as a Juvenile Probation Officer with the Florida Department of Juvenile Justice and during a portion of my employment I supervised a case load of juvenile sex offenders.

3. Your Affiant makes this Affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search an iCloud account assigned to the Apple ID, "[thewloungebar@gmail.com](mailto:thewloungebar@gmail.com)" and any iCloud accounts assigned to an iPhone with IMEI number "356707085318830" (hereinafter "ACCOUNTS") that are stored at premises owned, maintained, controlled, or operated by Apple Inc., as further described in Attachment A, for the things described in Attachment B.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit comes from my training and experience, my review of records, my direct observations, and through information obtained from other law enforcement officers.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. §§ 2251 and/or 2252 have been committed by an individual utilizing the ACCOUNTS. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits

of these crimes further described in Attachment B. I submit this application and affidavit in support of a search warrant authorizing a search of the ACCOUNTS, as further described in Attachments A and B, which are incorporated herein by reference.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States that has jurisdiction over the offense being investigated.”

### **PROBABLE CAUSE**

7. HSI received lead information from the Royal Canadian Mounted Police (“RCMP”) that originated from the Legal Department at Kik Interactive (“Kik”) indicating that between March 2019 and September 2019 four different Kik accounts were used to upload child pornography.

8. Information received from RCMP revealed that on March 28, 2019 at 05:56:31 UTC, a user of a Kik account associated with username alwayscravingyun uploaded an image of child pornography. Your Affiant reviewed the image and observed a prepubescent naked male child lying on his back with his legs up. The child’s arms were located at his sides and his fists were clenched next to each of his hips. The child’s genitals were exposed and an adult male’s genitals were touching the child’s anus. The Kik account used to upload the child pornography was registered on February 10, 2019 with an Apple iPhone. The letter A was registered to the account as the user’s first name and the name Will was registered to the account as the user’s last name. The email address registered to the account was 6ridosii.p@kulitlumpia.ml, which is considered to be a disposable email address and not traceable by law enforcement.

9. Information received from RCMP also revealed that on April 26, 2019 at 00:54:58 UTC, a user of a Kik account associated with username ajsmthlover uploaded a video that was flagged by Kik as abuse. Your Affiant reviewed the video and observed two minor male children that were dressed in what appeared to be school uniforms. One of the child's genitals were removed from his shorts and the other child rubbed the genitals and provided oral sex. The video is approximately 22 seconds long. The Kik account used to upload the video was registered on April 23, 2019 with an Apple iPhone. The letters AJ were registered to the account as the user's first name and the name Smith was registered to the account as the user's last name. The email address registered to the account was ajisbavk@yopmail.com, which is considered to be a disposable email address and not traceable by law enforcement.

10. Information received from RCMP revealed that on August 2, 2019 at 22:36:26 UTC, a user of a Kik account associated with username wllovemsmth uploaded an image of child pornography. Your Affiant reviewed the image and observed a naked prepubescent male child lying on a bed with his arms outstretched; the child's genitals were exposed and were the focus of the image. The Kik account used to upload the child pornography image was registered on July 24, 2019 at 00:53:14 UTC with an Apple iPhone. The letter W was registered to the account as the user's first name and the letter L was registered to the account as the user's last name. The email address registered to the account was [thewloungebar@gmail.com](mailto:thewloungebar@gmail.com).

11. Information received from RCMP revealed that on September 29, 2019 at 09:11:41 UTC, a user of a Kik account associated with username ajlovemsmth212 uploaded an image of child pornography. Your Affiant reviewed the image and observed a naked prepubescent male child lying on a bed with his arms outstretched; the child's genitals were exposed and were the focus of the image. The Kik account used to upload the child pornography was registered on September 28, 2019 with an Apple iPhone. The letters AJ was registered to the account as the

user's first name and the word Him was registered to the account as the user's last name. The email address registered to the account was AJlovemsmth212@gmail.com.

12. HSI determined that all four Kik accounts addressed above had logins that were associated with IP address 98.249.57.29 and that the internet service provider for that IP address was Comcast Cable Communications, LLC ("Comcast"). HSI submitted a DHS Summons to Comcast requesting subscriber records for IP address 98.249.57.29 assigned on 03-28-2019 at 05:56:31 UTC, 04-26-2019 at 00:54:58 UTC, 08-02-2019 at 22:36:26 UTC and 09-29-2019 at 09:11:41 UTC. Comcast could only identify a subscriber account associated with the requested IP address on 09-29-2019 at 09:11:41 UTC, as follows:

Subscriber Name:	Derek Jackson
Service/Billing Address:	511 Paul St, Harrisonburg, VA 22801-3229
Telephone #:	(540) 435-2435
Type of Service:	High Speed Internet Service
Account Number:	8299600710486531
Start of Service:	11-06-2018
Account Status:	Disconnected 10-31-2019
IP Assignment:	Dynamically Assigned
E-mail User Ids:	drjack0316

13. HSI submitted a DHS Summons to Verizon Wireless ("Verizon") requesting subscriber and toll records for phone number 540-435-2435, which was the phone number listed for the subscriber in the Comcast return information. Return information received from Verizon included the following:

Account Number-642183518-1  
Business Name-Rodney Williams and Associates  
Contact Name-Rodney Williams  
Address-511 Paul Street, Harrisonburg, VA 22801  
Effective Date-12/14/2017

14. Verizon reported the Device IMEI associated with this cellphone number was 352077090445125. HSI identified that IMEI 352077090445125 is assigned to a Samsung Galaxy Note 8 device, which is not the same type of device that was used to register the above-referenced

Kik accounts and which indicates that this was not the device and/or phone number used to create the above-referenced Kik accounts.

15. Verizon also reported additional phone numbers that were associated with this account, including but not limited to 540-820-7653.

16. HSI conducted open source record checks regarding the additional phone numbers assigned to the Verizon account. HSI identified phone number 540-820-7653 was listed as Rodney Williams's contact phone number on the Williams and Associates webpage. HSI submitted a DHS Summons to Verizon requesting subscriber and toll records for phone number 540-820-7653. Return information received from Verizon included the following:

Business Name-Rodney Williams and Associates  
Contact Name-Rodney Williams  
Address-511 Paul Street, Harrisonburg, VA 22801  
Effective Date-12/14/2017

17. Verizon reported the device IMEI number for phone number 540-820-7653 was **356707085318830**, which was issued to an Apple iPhone8. An Apple iPhone was the device used to register the above-referenced Kik accounts. Verizon reported IP sessions for internet activity that took place between March 4, 2019 and February 28, 2020 for the device assigned to phone number 540-820-7653. The mobile login IP addresses used by the device matched mobile IP addresses provided by Kik that were used to login into the above-referenced Kik accounts. The matching mobile IP addresses indicate the device associated with phone number 540-820-7653 and IMEI number **356707085318830** was used to access the Kik accounts that were used to upload child pornography. As discussed more below, because the device associated with phone number 540-820-7653 and IMEI number **356707085318830** is an Apple iPhone, there will be an Apple iCloud account associated with this device.

18. Further, HSI learned that the Harrisonburg Police Department (“HPD”), which is a member of the Northern Virginia Internet Crimes Against Children Task Force (“NOVA ICAC”), had an open child exploitation investigation pertaining to IP address 98.249.57.29, which is the same IP address associated with the above-referenced Kik accounts. HPD reported that they received a CyberTipline (“CT”) Report No. 57143145. The CT was created by the National Center For Missing and Exploited Children (“NCMEC”). The CT contained information submitted by Twitter, Inc./Vine.co (“Twitter”). The tip was in reference to at least one image that was identified as child pornography that was uploaded on October 14, 2019 and sent by a user utilizing Twitter username AJBoylv. This Twitter account was registered on August 18, 2019 at 21:58:38 UTC. Your affiant reviewed the image and observed a prepubescent male child lying in the back seat of a vehicle with his legs spread apart. The child was unclothed from the waist down, and his genitals were the focus of the image. The name AJBoylv was registered as the account’s screen/username, and the user provided the description “Fun Masc guy loving life. Gym sports bling. Into kink.” The email address registered to the Twitter account was [thewloungebar@gmail.com](mailto:thewloungebar@gmail.com), which is the same email address that was used while registering the Kik account associated with username wllovemsmth (see paragraph 10 above).

19. In April 2020, HSI executed a search warrant to Google for the email address **thewloungebar@gmail.com** as that email was associated with both a Kik account (username wllovemsmth) and a Twitter account (username AJBoylv) that was used to upload child pornography. Return information received indicated that on July 23, 2019 a new Gmail account was created, a new iCloud Apple ID (**thewloungebar@gmail.com**) was created, and the Apple ID **thewloungebar@gmail.com** was used to sign into iCloud on an Apple iPad.

20. This Court issued a search warrant for the gmail account [thewloungebar@gmail.com](mailto:thewloungebar@gmail.com). Although user attribution evidence from a

[thewloungebar@gmail.com](mailto:thewloungebar@gmail.com) search warrant return indicates that the email account belongs to Rodney Williams, Williams has claimed that the email account was available on an iPad that he let his guests and visitors use. Williams admitted creating the email account. When officers asked for the shared iPad and his iPhone, Williams claimed he had thrown away the iPad and he could not locate the iPhone. Therefore, law enforcement must try to access Williams' child pornography images or "stash" through other means, since the physical Apple-based devices may have been destroyed by Williams.

### **INFORMATION REGARDING APPLE ID AND iCloud**

21. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

22. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.



d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. Furthermore, through the iCloud service, Apple offers call history syncing as a convenience to their customers, so they can return calls from any of their devices. Apple stores these records in its iCloud service. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices,

or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

23. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

24. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

25. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and

utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

26. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

27. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

28. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by

Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

29. Moreover, based on my training and experience, I understand that an user of an Apple device will "back up" the contents of that device for various reasons, such as to protect the contents of the device if the device is damaged or before upgrading or switching devices. This "back up" is saved on the iCloud connected to the user's Apple ID and can often serve as a "snapshot" of the contents of a device on the date and time the Apple device is backed up to iCloud. Therefore, even if a user loses, damages, or disposes of an old Apple device, the contents of that device may still be available on iCloud.

30. Sexual exploitation of minors requires perpetrators to spend vast quantities of time building trust with their victims, including extensively communicating with them. Various methods are used in order to achieve this, such as texting, chatting, using FaceTime, etc. In this Affiant's training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and

how” of the criminal conduct under investigation, thus enabling law enforcement to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

31. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geolocation, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

32. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

33. Further, based on my training and experience, individuals who share child pornography often collect child pornography images for various reasons, such as to view at a later date or so that they have images they can use to trade for additional child pornography. Because iCloud contains cloud storage for photos and videos – storage that can be cheaply expanded by a user – the contents of the iCloud account may also contain other direct evidence of the suspected federal crimes.

34. Finally, this Affiant knows the suspect used various communication applications, such as Kik and Twitter. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

35. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In this Affiant's training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

36. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **CONCLUSION**

37. Based upon the foregoing, your Affiant submits that there exists probable cause to believe that the Apple iCloud accounts associated with the Apple ID "[thewloungebar@gmail.com](mailto:thewloungebar@gmail.com)" and the iPhone IMEI number 356707085318830 stored at the premises owned, maintained, controlled by Apple, Inc. contain evidence of violations of 18 U.S.C. §§ 2251 and/or 2252 and

therefore respectfully request that a warrant be issued for the search of the accounts described in Attachment A, for the search and seizure of the items more fully described in Attachment B.

**REQUEST FOR SEALING**

38. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.


**OATH**

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/Tami Ketcham  
Special Agent, ICE/HSI

Subscribed and sworn before me this 9<sup>th</sup> day of July 2020.



The Honorable Joel C. Hoppe  
United States Magistrate Judge  
Western District of Virginia

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to iCloud information associated with the Apple ID “[thewloungebar@gmail.com](mailto:thewloungebar@gmail.com)” and the iPhone IMEI number 356707085318830 (the “ACCOUNTS”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.



**ATTACHMENT B**

**Particular Things to Be Seized**

**I. Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”),

Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps

h. All records pertaining to the types of service used; and

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

## II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of **18 U.S.C. §§ 2251 and 2252**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Information, including but not limited to communication, media and transaction logs that were used to receive, distribute, and possess child pornography.
- b. Communication to and from Apple and other electronic services providers that can be used to receive, distribute, and possess child pornography.
- c. Possession, receipt, and production of child pornography.
- d. The identity of the person(s) who created and/or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- e. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- f. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- g. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- h. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communication, other records and information disclosed pursuant to this warrant in order to located evidence, fruits, and instrumentalities described in the warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.